REMARKS/ARGUMENTS

I. Status of Claims

Claims 1-20 stand rejected in the instant application. Claims 1-16 have been rejected under 35 USC § 102(e) as being anticipated by Meier, et al. (U.S. Publication 2004/0103282 A1), and claims 17-20 have been rejected under 35 USC § 103(a) as being unpatentable over Meier, et al., in view of Toyoshima (U.S. Publication 2002/0080741 A1).

Claims 1, 3, 5, 7, 9, 11, 13, 15, 17, and 19 have been amended. Support for these amendments is found throughout the originally submitted specification, claims and figures. Claims 2, 6, 10, 14, and 18, have been canceled without prejudice. No new claims have been added. Therefore it is respectfully submitted that no new matter has been added and the claims are now in condition for allowance.

II. Claim Rejections under 35 U.S.C. §102(e)

Claims 1-16

These claims stand rejected under 35 U.S.C. § 102(e) as being anticipated by Meier. In light of the current amendments, the Applicant respectfully traverses these rejections.

Claim 1 currently recites:

> A method, comprising:
>
> receiving, by an access point (AP) after distribution of a pairwise master key, a probe request;
>
> transmitting, by the AP, in response to the probe request, a probe response including an AP nonce generated by the AP; and
>
> receiving, by the AP, a pairwise master key request information element as a reassociate request from a user station that received the transmitted AP nonce, the pairwise master key request information element including the AP nonce, a user station nonce, and a message integrity code, wherein the message integrity code was computed using a message integrity code algorithm with a key confirmation key, the AP nonce, and the user station nonce, and wherein the key confirmation key was computed using a pseudo-random function algorithm with the pairwise master key, a media access control address of the AP, and a media access control address of the user station.

Therefore, claim 1 has been amended to clearly include the recitations that the pairwise master key request information element include the AP nonce, a user station nonce, and a message integrity code. Additionally, the claim has been amended to include the clarifying features that

the message integrity code is computed using a message integrity code algorithm with a key confirmation key, the AP nonce, and the user station nonce, and further, that the key confirmation key is generated using a pseudo random function algorithm with the pairwise master key, a media access control address of the AP and a media access control address of the user station.

In contrast, Meier teaches a new key hierarchy in which session keys are maintained by a subnet context manager ("SCM"). More specifically, the key hierarchy defines keys established on a successful authentication as network session keys ("NSK"). The NSK is used to generate a "key request key" ("KRK") and a "base transient key" ("BTK"). The BTK, in turn, serves as the base key from which pairwise transient keys ("PTK") are derived. *Meier*, p.6 paragraph [0181]. As is known in the art, the PTK is divided into separate keys such as a key confirmation key and a key encryption key, among others. Therefore, due to the hierarchy taught by Meier, it is axiomatic that Meier fails to teach computing the key confirmation key in the manner required by claim 1. Rather, Meier teaches, computing the PTK (which necessarily includes the KCK and the KEK) with a BTK (base transient key), RN (a rekey request sequence number), and a BSSID (a basic service set identifier). Therefore, for at least this reason, claim 1 is allowable over the Meier.

Additionally, Meier fails to teach computing a message integrity code as required by now amended claim 1. The Examiner previously relied on the user station transmitting a message integrity code based on the key request key. *Meier*, Fig. 8, Arrow 19. The Applicant notes, however, that given the clarifying amendment, Meier fails to anticipate the claim because there is no teaching that the MIC is computed using the various keys within the PTK (i.e., KCK, KEK), as is now required. Therefore, for at least this additional reason, claim 1 is allowable over Meier.

Furthermore, it would not have been obvious to one or ordinary skill in the art given the teachings of Meier to arrive at the features of claim 1 because Meier expressly teaches away the instant method of deriving PTK's (i.e. the KCK and KEK). For at least these reasons, claim 1 is allowable over Meier. The Applicant respectfully requests the Examiner withdraw their rejection of the claim.

Claims 3 and 4 depend or indirectly from independent claim 1 thereby incorporating its recitations. Therefore, for at least the same reason that claim 1 is allowable over Meier, claims 3 and 4 are similarly allowable.

Independent claims 5, 9, and 13 all contain recitations similar to that of claim 1. Therefore, for at least the same reasons that claim 1 is allowable, claims 5, 9, and 13 are similarly allowable.

Dependent claims 7-8, 11-12, and 15-16 all depend either directly or indirectly from independent claims 5, 9, and 13. Therefore, for at least the same reasons that claims 5, 9, and 13 claims 7-8, 11-12, and 15-16 are similarly allowable.

While allowable due to its dependence on independent claim 1, the Applicant notes that claim 3 is independently allowable over Meier.

Claim 3 currently recites:

> A method as claimed in claim 1, further comprising:
>
> generating, by the AP, a pairwise master key response element based on the user station nonce and an additional message integrity code, the additional message integrity code being computed using the message integrity code algorithm with a key encryption key, the probe response, and the pairwise master key request information element, and wherein the key encryption key is computed using the pseudo random function algorithm with the pairwise master key, the media access control address of the AP, and the media access control address of the user station; and
>
> transmitting, by the AP, the pairwise master response element as a reassociation response.

Therefore, claim 3 clearly includes the recitations that the additional message integrity code be computed using a message integrity code algorithm with a key encryption key, the probe response and the pairwise master key. Additionally, the Key encryption key ("KEK") is computed using a PRF algorithm with the PMK, the media access control ("MAC") address of the AP, and the MAC address of the user station.

In contrast, Meier teaches that the KEK (i.e., the PTK) is computed using various other keys which are unique to the hierarchy disclosed in Meier, such as the BTK. *Meier*, Figure 1. Therefore, Meier fails to teach each and every recitation of claim 3 as is required under 35 U.S.C. § 102. Consequently, the Applicant respectfully asserts that claim 3 is allowable for at

least this additional reason. The Applicant requests that the Examiner withdraw their rejection to the claim.

Dependent claims 7, 11, and 15 contain similar recitations to that of claim 3. Therefore they are similarly allowable for at least the same additional reason. Therefore, it is respectfully submitted that claims 1, 3-5, 7-9, 11-13, and 15-16 are allowable.

III. Claim Rejections under 35 U.S.C. §103(a)

In the subject office action, claims 17-20 were rejected as being unpatentable over Meier et al. in view of Toyoshima.

Claim 17 is directed to an apparatus that includes features similar to those discussed with reference to clams 1. Furthermore, it is respectfully submitted that Toyoshima does not make up for the lack of teaching in Meier, et al. Rather, Toyoshima was merely relied upon for its teaching of an "omni-directional" antenna.

Therefore, it is respectfully submitted that claim 17 is allowable over Meier either alone or in combination with Toyoshima. It is respectfully requested that the Examiner withdraw their rejection under 35 U.S.C. § 103. Dependent claims 19-20 rely either directly or indirectly on claim 17 thereby incorporating its limitations. Therefore, for at least the same reason that claim 17 is allowable, it is respectfully submitted that claims 19-20 are also allowable.

In addition to its dependence on claim 17, claim 19 is independently allowable over the cited art. Claim 19 includes recitations similar to those discussed above with reference to claim 3. Because Toyoshima does not cure the additional deficiencies of Meier, claim 19 is allowable for at least this additional reason.

Accordingly, it is respectfully submitted that Claims 17-20 are also allowable.

IV. Conclusion

In view of the foregoing, Applicants submit all pending claims, specifically, claims 1, 3-5, 7-9, 11-13, 15-17, and 19-20 are in condition for allowance. The Examiner is invited to call the undersigned at (503) 796-2408 regarding any inquiry concerning this communication. Issuance of a Notice of Allowance is respectfully requested.

The Commissioner is hereby authorized to charge shortages or credit overpayments to Deposit Account No. 500393.

Respectfully submitted,

SCHWABE, WILLIAMSON & WYATT, P.C.

Dated: 12/12/2007

/Rob McDowell/
Rob D. McDowell, Reg. No. 59,062

Pacwest Center, Suite 1900
1211 SW Fifth Avenue
Portland, Oregon 97204
Telephone: 503-222-9981